UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

IN RE: MOVEIT CUSTOMER DATA SECURITY BREACH LITIGATION This Document Relates To: ALL CASES	MDL No. 1:23-md-03083-ADB-PGL

MDL Order No. 19
(Order on Defendants Rule 12(b)(1) Motion to Dismiss for Lack of Article III Standing)

Before the Court is an omnibus Motion to Dismiss for lack of Article III standing filed by the Defendants' liaison committee in the multidistrict litigation ("MDL") arising from the MOVEit Transfer software data breach. [ECF No. 1114]; see also [ECF No. 1114-1 ("Motion" or "Mot.")]. Having reviewed Plaintiffs' Omnibus Statement of Additional Pleading Facts, [ECF No. 908 ("Common Complaint" or "Common Compl.")], Defendants' Motion, Plaintiffs' Opposition, [ECF No. 1194 ("Opposition" or "Opp'n"), Defendants' Reply, [ECF No. 1233 ("Reply")], Plaintiffs' Sur-Reply, [ECF No. 1256 ("Sur-Reply")], the record, applicable law, and the parties' presentation at oral argument, see [ECF No. 1269 ("Oral Argument Transcript" or "Oral Arg. Tr.")], the Court hereby orders that the Motion is **GRANTED IN PART** and **DENIED IN PART** as set forth herein and in the Appendix.

The question before the Court is whether the factual asseverations in the Common Complaint are sufficient to make out a plausible claim for relief that falls within the subject matter jurisdiction of this Court. As discussed below, on the issue of standing the outcome is largely dictated by the First Circuit's decision in Webb v. Injured Workers Pharmacy, LLC, 72 F.4th 365 (1st Cir. 2023). To summarize the key conclusions in this decision: Plaintiffs have

plausibly alleged that the data breach at issue in this case amounted to a single breach and have plausibly alleged that the posting of exfiltrated confidential information (PII) to the web caused some Plaintiffs to suffer actual harms that are traceable to that breach. It follows, in keeping with Webb, that this Court has jurisdiction over the claims of those Plaintiffs who allege that the breach exposed them to a substantial risk of harm and who further allege that such risk caused them to incur costs by way of mitigation and to suffer emotional harms. Whether Plaintiffs' claims ultimately have merit is a question for another day. The Court decides today only that (most) Plaintiffs have standing to pursue their claims.

I. Background

a. Relevant Facts

Except where specifically noted, the following facts are drawn from the well-pleaded allegations in the Common Complaint, which the Court takes as true and from which the Court draws all reasonable inferences in Plaintiffs' favor. See Webb v. Injured Workers Pharmacy, LLC, 72 F.4th 365, 371 (1st Cir. 2023) (quoting In re Evenflo Co., Inc., Mktg., Sales Pracs. & Prods. Liab. Litig., 54 F.4th 28, 34 (1st Cir. 2022)).

This MDL arises from a data breach targeting MOVEit Transfer, a secure file-transfer software developed by Progress Software Corporation ("Progress"), that took place in May and June 2023 (the "Data Breach"). [Common Compl. ¶¶ 1–3, 150, 194]. MOVEit Transfer is designed to be installed on the servers of Progress customers, who are "primarily businesses, organizations, and governmental entities," including "healthcare companies, healthcare benefits providers," "banking and financial institutions, pension benefit plans, health insurers, colleges and universities, state governments and local municipalities, biotech companies, charter schools, credit unions, emergency services corporations, IT services companies, marketing companies,

social service providers, [and] software and technology companies." [Id. ¶¶ 15–17, 21, 191–92]. A Russian cybercriminal group called Cl0p[1] exploited security vulnerabilities endemic to the code of "[a]ll versions of MOVEit Transfer" and exfiltrated personally identifiable information ("PII") and, in some cases, protected health information ("PHI") from more than 2,600 entities, affecting more than 93 million individual records as of January 2024. [Id. ¶¶ 90, 132, 151, 193–96].

Plaintiffs allege that after the Data Breach, Cl0p attempted to extort Progress customers by demanding payment in exchange for the return of the exfiltrated information. [Common Compl. ¶¶ 92, 199, 207–14]. Hundreds of direct users of MOVEit Transfer, as well as Vendors, Vendor Contracting Entities ("VCEs"), and Vendor Contracting Entity Customers ("VCECs"), who Cl0p says rebuffed or ignored the hackers' ransom demands have had the stolen data published on the dark or clear web, although Plaintiffs do not allege which customers, if any, paid Cl0p. [Id. ¶¶ 210–12]. Plaintiffs maintain that both Progress and the non-Progress Defendants failed to take reasonable precautions both before and during the Data Breach and that these alleged failures resulted in a variety of injuries, see [id. ¶¶ 252–71, 282–468], including fraud, [id. ¶ 279], as well as a substantial future risk that Plaintiffs' data will be misused, [id. ¶¶ 235, 246–51, 281].

[1] Cl0p is also referred to in the cybersecurity community as Threat Actor 505 or "TA505," and in some materials, "Cl0p" is used interchangeably to describe both (1) the underlying ransomware program deployed by TA505 and (2) the actors associated with TA505 who deploy the ransomware. See, e.g., Cybersecurity & Infrastructure Sec. Agency, #Stop Ransomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability, Cybersecurity Advisory: Alert AA23-158A, (Jun. 7, 2023), https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a. Consistent with the parties' filings, all references to "Cl0p" in this order refer to the hacking group.

b. Procedural History

Individual plaintiffs have filed more than 300 cases against various configurations of Defendants, including Progress, Direct Users, Vendors, VCEs, and VCECs. In October 2023, the Joint Panel on Multidistrict Litigation ordered the creation of this MDL and began transferring cases to the District of Massachusetts. See [ECF No. 2 ("Transfer Order") (J.P.M.L. Oct. 4, 2023)].

With the consent of the parties and largely in line with their proposal on briefing threshold issues relating to subject-matter jurisdiction, the Court entered a briefing schedule for some threshold issues, including motions for dismissal for lack of Article III standing. See [ECF No. 874 ("MDL Order No. 13")]; [ECF No. 851 ("Joint Proposal Regarding Briefing of Threshold Issues")]. Pursuant to that order, Plaintiffs filed an amended complaint of common factual allegations (the "Common Complaint") on May 24, 2024. See generally [Common Compl.]. The Common Complaint supplements the allegations in the individual complaints consolidated before the Court by setting forth "a set of common factual allegations that Plaintiffs contend are relevant to the standing analysis for all parties including, by way of example, information newly discovered on CL0P's website and the dark web." [ECF No. 851]; see also [ECF No. 874 at 2 n.1]. On July 23, 2024, Defendants filed an omnibus motion to dismiss for lack of Article III standing. [Mot.] Plaintiffs opposed on September 5, 2024, [Opp'n], Defendants replied on September 26, 2024, [Reply], and with the Court's leave, Plaintiffs sur-replied on October 7, 2024, [ECF No. 1254]; [Sur-Reply]. The Court heard oral argument on October 9, 2024. [ECF No. 1269, 1271].

II. Legal Standard

"On a motion to dismiss for lack of subject matter jurisdiction . . . , 'the party invoking the jurisdiction of a federal court carries the burden of proving its existence.'" Equal Means Equal v. Dep't of Educ., 450 F. Supp. 3d 1, 4–5 (D. Mass. 2020) (quoting Murphy v. United States, 45 F.3d 520, 522 (1st Cir. 1995)); see also Katz v. Pershing, LLC, 672 F.3d 64, 75 (1st Cir. 2012) ("Article III standing presents a question of justiciability; if it is lacking, a federal court has no subject matter jurisdiction over the claim."). Dismissal is appropriate only when the well-pleaded allegations in the complaint, taken as fact and given all reasonable inferences, do not support a finding of federal subject matter jurisdiction.[2] Fothergill v. United States, 566 F.3d 248, 251 (1st Cir. 2009).

III. Discussion

a. Standing

Article III of the Constitution limits the subject-matter jurisdiction of federal courts to adjudicating "actual cases and controversies." Kerin v. Titeflex Corp., 770 F.3d 978, 981 (1st Cir. 2024) (citing Warth v. Seldin, 422 U.S. 490, 498 (1975)). In so doing, the Constitution "restricts [federal courts] to the[ir] traditional role . . . , which is to redress or prevent actual or imminently threatened injury to persons caused by private or official violation of law." Summers v. Earth Island Inst., 555 U.S. 488, 492 (2009). "One element of the case-or-controversy requirement is that plaintiffs must establish that they have standing to sue." Clapper v. Amnesty

[2] The Court, however, is not restricted to the four corners of the Complaint and "may consider whatever evidence has been submitted," including exhibits. Aversa v. United States, 99 F.3d 1200, 1210 (1st Cir. 1996); see also Torres-Negron v. J & N Records, LLC, 504 F.3d 151, 163 (1st Cir. 2007).

Int'l USA, 568 U.S. 398, 408 (2013) (internal quotation marks omitted) (quoting Raines v. Byrd, 521 U.S. 811, 818 (1997)).

"To satisfy this standing requirement, a plaintiff must sufficiently," meaning plausibly, "plead three elements: injury in fact, traceability, and redressability." Kerin, 770 F.3d at 981 (citing Lujan v. Defs. of Wildlife, 504 U.S. 555, 560–61 (1992)); see also Gustavsen v. Alcon Lab'ys, Inc., 903 F.3d 1, 7 (1st Cir. 2018) ("[Courts] apply the same plausibility standard used to evaluate a motion under Rule 12(b)(6) [when ruling on a Rule 12(b)(1) motion]."). In other words, "a plaintiff must show an injury in fact caused by the defendant and redressable by a court order." Webb, 72 F.4th at 372 (quoting United States v. Texas, 599 U.S. 670, 676 (2023)). "In applying the plausibility standard required at the motion to dismiss stage," the Court "draw[s] on [its] judicial experience and common sense . . . [and] read[s] the complaint as a whole." Id. at 373 (omission and third alteration in original) (quoting Evenflo, 54 F.4th at 39).

Defendants mainly challenge whether plaintiffs' allegations satisfy the injury-in-fact and traceability requirements for standing.[3] See [Mot. at 16–45]. Accordingly, the Court's analysis focuses on those two elements.

[3] Defendants touch on Plaintiffs' standing to seek injunctive relief (albeit for the first time in their reply brief). [Reply at 18]. The Court agrees that many of Plaintiffs' claims for injunctive relief require dismissal because prospective remedies targeting the named Defendants cannot address the risk of future harm caused by the Data Breach. See Webb, 72 F.4th at 378. Plaintiffs' otherwise cognizable injuries would be redressable through monetary relief and thereby satisfy the redressability requirement of Article III standing. See id. at 377 ("[M]onetary relief would compensate [the plaintiffs] for their injur[ies], rendering the injur[ies] redressable." (second, third, and fourth alterations in original) (quoting Evenflo, 54 F.4th at 41)). The parties' appendices show agreement on the cases involving nonjusticiable claims for injunctive relief, which are specifically identified in the appendix following this order.

b. Injury in fact

To sufficiently plead injury in fact, a plaintiff must plausibly allege "an invasion of a legally protected interest which is (a) concrete and particularized, and (b) 'actual or imminent, not conjectural or hypothetical." Lujan, 504 U.S. at 560 (citations omitted). As the First Circuit has explained, "'[t]raditional tangible harms, such as physical harms and monetary harms,' are 'obvious[ly]' concrete." Webb, 72 F.4th at 372 (second alteration in original) (quoting TransUnion LLC v. Ramirez, 594 U.S. 413, 425 (2021)). "'Concrete' is not, however, necessarily synonymous with 'tangible.'" Spokeo, Inc. v. Robins, 578 U.S. 330, 340 (2016). To the contrary, "[i]ntangible harms can also be concrete, including when they 'are injuries with a close relationship to harms traditionally recognized as providing a basis for lawsuits in American courts,' such as 'reputational harms, disclosure of private information, and intrusion upon seclusion.'" Webb, 72 F.4th at 372 (quoting TransUnion, 594 U.S. at 425). Still, a sufficiently close relationship "does not require an exact duplicate" to a common-law harm. TransUnion, 594 U.S. at 424.

The inquiry for determining whether an increased risk of future harm is "concrete" for purposes of Article III standing turns, in part, on the type of relief a plaintiff seeks. "[A] material risk of future harm [alone] can . . . satisfy the concrete-harm requirement" for purposes of injunctive relief, Webb, 72 F.4th at 372 (first alteration in original) (quoting TransUnion, 594 U.S. at 435), whereas to pursue damages, "plaintiffs must [also] demonstrate a separate concrete harm caused 'by their exposure to the risk itself.'" Id. (quoting TransUnion, 594 U.S. at 437). In other words, risk-based standing to seek damages "involve[s] two injuries: (1) a possible future injury that may or may not happen (i.e., the harm threatened); and (2) a present injury that is the cost or inconvenience created by the increased risk of the first, future injury (e.g., the cost of

mitigation)." Kerin, 770 F.3d at 981–82. Still, "not all risks constitute injury," and the First Circuit has urged "caution" in cases involving standing based on risk. Id. at 982–83. "Where . . . Plaintiffs have not shown an imminent risk of [injury], prophylactic costs to mitigate such a risk do not constitute an independent injury sufficient to support standing." Taylor v. UKG, Inc., 693 F. Supp. 3d 87, 100 (D. Mass. 2023) (citation omitted).

The standing inquiry in this case is largely controlled by the First Circuit's decision in Webb v. Injured Workers Pharmacy. See 72 F.4th at 371–78. Two putative class plaintiffs, Webb and Charley, were patients of Injured Workers Pharmacy ("IWP"), a "home-delivery pharmacy service." Id. at 369. IWP suffered a data breach in January 2021, in which hackers accessed 75,000 patients' personally identifiable information ("PII"), including names and Social Security numbers. Id. at 370. Webb and Charley filed a class-action complaint against IWP seeking damages and injunctive relief for claims of negligence, breach of implied contract, unjust enrichment, invasion of privacy, and breach of fiduciary duty. Id. at 370–71.

Webb alleged that her PII had been used to file a fraudulent tax return for the year 2021 (i.e., filed in 2022, after the IWP data breach), which required her to "'expend[] considerable time' communicating with the Internal Revenue Service ('IRS') to resolve issues associated with [the] false return." Webb, 72 F.4th at 370 (quoting operative complaint). Webb also alleged that after receiving notice that her PII had been stolen in the IWP breach, she (a) "fear[ed] for her personal financial security and [for] what information was revealed in the [d]ata [b]reach," (b) "spent considerable time and effort monitoring her accounts to protect herself from . . . identity theft," and (c) "experience[ed] [ongoing] feelings of anxiety, sleep disruption, stress, and fear." Id. (omission and second, third, and fourth alterations in original) (quoting operative complaint). Charley alleged that after learning her PII had been affected, she too "fear[ed] for her personal

financial security," "expend[ed] considerable time and effort monitoring her accounts to protect herself from . . . identity theft," and "experienc[ed] feelings of rage and anger, anxiety, sleep disruption, stress, fear, and physical pain." Id. (omission and alterations in original) (quoting operative complaint). Charley did not allege that PII stolen in the IWP breach had been misused. See id. at 374 ("The complaint does not allege actual misuse of Charley's PII."). IWP filed a motion to dismiss for lack of standing,[4] which the district court granted, concluding that neither Webb nor Charley had plausibly alleged a concrete injury. Id. at 371.

The First Circuit reversed, concluding that both plaintiffs satisfied the concreteness requirement. First, with respect to Webb, "the complaint's plausible allegations of actual misuse of Webb's stolen PII to file a fraudulent tax return suffice[d] to state a concrete injury under Article III." Webb, 72 F.4th at 373. Webb's allegation that someone filed a fraudulent tax return in her name distinguished her pleadings from earlier First Circuit data breach cases in which the plaintiff had not alleged that anyone "ha[d] acted on the ill-gotten information." Id. (emphasis omitted) (distinguishing Katz, 672 F.3d at 80); see also In re Equifax Inc. Customer Data Sec. Breach Litig., 999 F.3d 1247, 1262 (11th Cir. 2021) (concluding that "identity theft and damages resulting from such theft" counted as concrete injuries); Attias v. CareFirst, Inc., 865 F.3d 620, 627 (D.C. Cir. 2017) ("Nobody doubts that identity theft . . . constitute[s] a concrete and particularized injury.").

Second, even though "the complaint d[id] not allege actual misuse of Charley's PII," she too satisfied the concrete-injury requirement. Webb, 72 F.4th at 374. "[I]n light of the plausible

[4] Although IWP also moved for dismissal under Rule 12(b)(6), the First Circuit declined to address whether dismissal for failure to state a claim was appropriate as the district court had not yet addressed that ground. Webb, 72 F.4th at 371, 378–79.

allegations of some actual misuse,"[5] the "complaint plausibly allege[d] a concrete injury in fact based on the material risk of future misuse of Charley's PII and a concrete harm caused by exposure to this risk." Id. As this Court previously explained in Taylor, the future-injury analysis in Webb proceeded in two steps, 693 F. Supp. 3d at 98–100, corresponding to what the First Circuit in Kerin called the "harm threatened" in the future because of the defendant's conduct, and the present injury caused by the "cost of mitigation," 770 F.3d at 982.

To examine "the harm threatened," the First Circuit in Webb considered three factors that have been widely applied in other circuits, and concluded that each of these factors weighed in favor of finding an injury in fact.[6] 72 F.4th at 375. First, "data compromised in a targeted attack is more likely to be misused." Id. In Webb, this factor weighed in favor of finding injury in fact where the complaint alleged that the data breach was an "attack by 'cybercriminals' who 'infiltrated IWP's patient records systems' and 'stole[] PII.'" Id. at 375–76 (alteration in original) (quoting operative complaint). Second, if "at least some information stolen in a data breach has already been misused," then it is more "likely that other portions of the stolen data will be similarly misused." Id. at 376. Where the Webb complaint "allege[d] that at least some of the stolen PII ha[d] already been misused to file a fraudulent tax return in Webb's name," this too weighed in favor of injury in fact. Id. Third, "the risk of future misuse may be heightened where the compromised data is particularly sensitive." Id. Regarding this third factor, the court noted, "[n]aturally, the dissemination of high-risk information such as Social Security numbers

[5] Charley did not argue that "the exposure of [her] PII in the breach was itself an intangible harm sufficient to confer standing." Webb, 72 F.4th at 374 n.5.

[6] As the Court stressed in Taylor, the Webb factors "'are neither exclusive nor necessarily determinative, but they do provide guidance.'" Taylor, 693 F. Supp. 3d at 98 (quoting Webb, 72 F.4th at 375).

and dates of birth — especially when accompanied by victims' names — makes it more likely that those victims will be subject to future identity theft or fraud." Id. (quoting McMorris v. Carlos Lopez & Assocs., LLC, 995 F.3d 295, 302 (2d Cir. 2021)). The Webb complaint alleged that the data stolen from IWP was particularly sensitive, including "patients' names and [S]ocial [S]ecurity numbers." Id. (alterations in original). Thus, the Webb Court concluded in that case that "the totality of the complaint plausibly allege[d] an imminent and substantial risk of future misuse of the plaintiffs' PII."[7] Id.

Webb offers a useful illustration of the analysis required when determining when mitigation costs will satisfy the injury-in-fact requirement. The starting point for this analysis is TransUnion's requirement that to "establish standing to pursue damages, the complaint must also plausibly allege a separate concrete, present harm caused 'by [the plaintiffs'] exposure to [this] risk [of future harm].'" Webb, 72 F.4th at 376 (alterations in original) (quoting TransUnion, 594 U.S. at 436). On that foundation, the court in Webb found that the allegations met this standard "based on the allegations of the plaintiffs' lost time spent taking protective measures that would otherwise have been put to some productive use." Id. Specifically, the court found that "'opportunity costs' and 'lost wages' associated with 'the time and effort expended addressing . . . future consequences of the [d]ata [b]reach'" were "equivalent to a monetary injury, which is indisputably a concrete injury." Id. (alterations in original). And since "this alleged injury was a response to a substantial and imminent risk of harm," the plaintiff's

[7] Although Webb's holding with respect to future misuse appears to apply to both Webb and Charley, as evidenced by the First Circuit's use of the plural possessive to refer to a risk of future misuse of "plaintiffs' PII," Webb, 72 F.4th at 376, the Court focuses on the applicability of this holding to Charley. The Court notes that, once the First Circuit determined that Webb had Article III standing based on her allegations of actual misuse, it was unnecessary to decide whether she could also have asserted standing based on a risk of future injury.

mitigation costs differed from "case[s] where . . . plaintiffs seek to 'manufacture standing by incurring costs in anticipation of non-imminent harm.'" Id. (quoting Clapper, 568 U.S. at 422).

Applying Webb to the allegations in this MDL, the Court concludes that, at the motion to dismiss stage, the plaintiffs have sufficiently alleged: that they face a material risk of future harm; that most plaintiffs have suffered a present injury as a consequence of that risk; and that the future risk of harm affecting most plaintiffs is traceable to the Defendants' actions in connection with the data breach.

c. Material Risk of Future Harm

The Court concludes that the balance of the three Webb factors weighs in favor of finding injury in fact based on exposure to a "material risk of future harm." 72 F.4th at 371 (quoting TransUnion, 141 S. Ct. at 2210).

i. Factor One: Whether the data was stolen in a targeted attack.

The Common Complaint alleges that Cl0p designed code to exploit latent vulnerabilities in the operative versions of MOVEit Transfer installed on its customers' servers. [Common Compl. ¶¶ 135–44]. The Court finds, and Defendants do not contest, that these allegations adequately plead that Plaintiffs' data was "exposed in a targeted attack rather than inadvertently." Webb, 88 F.4th at 375.

Defendants nonetheless contend that the allegations fall short of Webb's requirements. In particular, Defendants argue that the Common Complaint lacks allegations that "Cl0p's motive was to misuse any individual's data," which, Defendants maintain, "was the case in Webb." [Mot. at 21–22]. Rather, Defendants contend Plaintiffs' allegation that Cl0p engaged in a ransomware attack means the hackers' "motive was not to use individuals' data itself to engage in identi[t]y theft or other fraud or even to post individuals' data for sale, but rather to turn a

profit by threatening victim organizations with ransom demands." [Id. at 22]. During oral argument, Defendants additionally argued that given the nature of the attack, Plaintiffs associated with non-Progress defendants who paid Cl0p's ransom face no future risk of harm at all as a result of making the demanded payment. [Oral Arg. Tr. at 45:1–50:1].

Defendants' arguments on this point raise issues that may be relevant to a finder of fact. It cannot be said, however that, as a matter of law, someone whose data has been stolen by pirates has nothing to worry about based on the surmise that a demand for ransom obviates the risk of the data being used to harm. The allegations in the Common Complaint are sufficient to plausibly claim harm, and thus standing. Plaintiffs allege that where no ransom has been paid, Cl0p has "threat[ened] to publish the data on the dark or clear web for further exploitation or sale." [Common Compl. ¶ 216]; see also [id. ¶¶ 177–84 (describing ransom threats sent to MOVEit Transfer users)]. Plaintiffs also argue that payment of a ransom does not negate standing based on an increased risk of harm because there is no way to determine whether Cl0p or a third party has misused the data (or will do so in the future) despite having their ransom demand met. [Id. ¶¶ 219–22]; see also [Oral Arg. Tr. at 47:3–10]. The Court agrees with Plaintiffs that a ransomware attack, even when a payment has been made, does not render it per se implausible that Plaintiffs face an ongoing risk of harm. Cf. Kaufman v. CVS Caremark Corp., 836 F.3d 88, 96 (1st Cir. 2016) (denying a Rule 12(b)(6) motion because studies cited in the complaint did not "render implausible [plaintiff's] allegation that substantiation for [misleading statements made by defendant] d[id] not exist"). Plaintiffs allege that an enormous volume of data has been published on the clear and dark web, and the Court cannot, based on the pleadings alone, determine whether certain defendants paid ransoms and whether this would affect liability or exposure. Clemens v. ExecuPharm Inc., 48 F.4th 146, 157 (3d Cir. 2022)

(finding that plaintiffs subject to ransomware attack established standing when facts supported that attacker "launched a sophisticated phishing attack to install malware, encrypted the data, held it for ransom, and published it"). As the Court has previously explained, although a ransomware attack may "cut against standing," Scifo v. Alvaria, Inc., No. 23-cv-10999, 2024 WL 4252694, at *5 n.8 (D. Mass. Sept. 20, 2024), cases that have found lack of standing based on a ransomware attack typically involve concessions (explicit or implied) in the pleadings that a ransom was paid. See, e.g., In re Practicefirst Data Breach Litig., No. 21-cv-00790, 2022 WL 354544, at *5 (W.D.N.Y. Feb. 2, 2022), report and recommendation adopted, 2022 WL 3045319 (W.D.N.Y. Aug. 1, 2022). Here, as in Scifo, the Common Complaint lacks any allegations that any ransom was paid by any Defendant. See 2024 WL 4242694, at *5 n.8. "Given that Plaintiffs have pleaded that their data was subject to a third-party attack and that the data could be valuable on the dark web, taking all facts in the light most favorable to Plaintiffs on a motion to dismiss, the Court will consider this factor as weighing in favor of standing" notwithstanding the fact that Cl0p deployed a ransomware attack. Id.

ii. Factor Two: Whether some of the information stolen has already been misused.

The core of the parties' dispute centers on the legal adequacy of Plaintiffs' allegations that portions of the data stolen by Cl0p have already been misused. The parties agree that some, but not all, of the individual plaintiffs in the MDL have adequately pled that their data has been misused, particularly through financial fraud, although they disagree as to just how many. Compare [Mot. at 19 (Defendants suggesting that "only about 30 [Plaintiffs] allege arguably plausible claims of actual misuse" (emphasis omitted)]; with, e.g., [Opp'n at 17 (Plaintiffs

contending that "[a]t least 157 Plaintiffs specifically plead actual fraudulent or attempted misuse of their Private Information after it was accessed and stolen in the Data Breach")].

Plaintiffs' maintain that plausible allegations of misuse, without regard to "[w]hether that number is 'only about 30,' or is instead correctly calculated at 157," means that "[a]ll Plaintiffs have standing here because their data was stolen by the same criminals who misused other . . . data to perpetrate fraud," [Opp'n at 17]. In their view, because the data was stolen by a single threat actor, "there is now only one repository of stolen information in the hands of Cl0p, and it is this repository from which the risk of future misuse emanates." [Id. at 25]. As Plaintiffs argue:

> For purposes of establishing the material future risk that the bad actor will misuse the stolen data, what matters is that all of the data stolen in the MOVEit Data Breach was stolen by the same bad actors, at the same time (exploiting the same vulnerability), and for the same purpose. Under these facts, applying the reasoning of Webb, the material risk of future misuse is shown for the entire repository of stolen data, regardless of which Defendant held the bit of data that was misused for any particular Plaintiff. The data was stolen from a separate repository for each Defendant, but it is all in one repository now — the one maintained by the bad actors — and that is what matters for purposes of assessing future risk of misuse.

[Opp'n at 4].

Defendants respond that "just because some individual MOVEit Incidents involving certain Defendants resulted in claims of misuse does not mean those misuse claims can be imputed to all of the MOVEit Incidents that were allegedly related to the MOVEit vulnerability." [Mot. at 23]. At least in part, Defendants' position seems premised on the view that the MOVEit data breach constitutes a large number of discrete cybersecurity incidents, rather than a single attack. See [id. ("That the outcome of one MOVEit Incident allegedly resulted in actual misuse of data says nothing about the risk to Plaintiffs impacted by a totally separate MOVEit Incident.")]. As they explained at oral argument, their position is that a plausible allegation that a

Genworth plaintiff has suffered actual harm does not support inferring an increased risk that a PBI plaintiff will also suffer actual harm. [Oral Arg. Tr. at 68:2–7].

The Court agrees with Defendants that Webb is not on all fours with this MDL. To be sure, Webb held that the fact that "at least some information stolen in a data breach has already been misused . . . makes it [more] likely that other portions of the stolen data will be similarly misused." 72 F.4th at 376. In that case, however, both lead plaintiffs allegedly suffered data loss due to a breach of a single entity, see id. at 370. In that respect, the circumstances in Webb differ markedly from the allegations in this MDL, where hundreds of lead plaintiffs allegedly suffered data loss through a software breach (or breaches) that affected hundreds of entities, see [Common Compl. ¶ 209].

Nevertheless, despite these factual differences and the possibility that parts of this litigation will doubtless focus more on single-plaintiff classes, the Common Complaint sufficiently alleges that, like the incident in Webb, the MOVEit breach constitutes a single cybersecurity incident.[8] The allegations consistently characterize the incident as one data breach, rather than multiple breaches associated with each Progress customer. Specifically, the Common Complaint alleges the MOVEit Incident was "a massive data breach" perpetrated by a single threat actor, Cl0p and that Cl0p exploited a zero-day vulnerability common to MOVEit Transfer software used by all customers to "simultaneously" attack thousands of MOVEit customer servers at once. [Common Compl. ¶¶ 1, 96–135]. Also, according to the Common Complaint, the LEMURLOOT vulnerability allowed Cl0p "to simultaneously attack thousands of MOVEit

[8] The scope of the breach presents a question of fact that, at this stage, turns on Plaintiffs' well-pleaded allegations. As noted earlier, the Court is bound to "accept as true all well-pleaded factual averments" in the Common Complaint "and indulge all reasonable inferences therefrom" in their favor. Gustavsen, 903 F.3d at 7 (citation omitted); see also Taylor, 693 F. Supp. 3d at 97.

Transfer servers and steal troves of data in a relatively short time before detection." [Id. ¶ 144]. For example, "[b]y December 20, 2023, over 2,600 organizations had been named as victims of the Data Breach." [Id. ¶ 183 (emphasis added)]. The Common Complaint also sets forth detailed allegations describing how Progress (not its individual customers) worked to patch the vulnerabilities. [Id. ¶ 156–66]. Taking these well-pleaded allegations as true at this stage, as it must, the Court finds that at least for current purposes, the Common Complaint describes a single data breach targeting software with multiple users.[9]

Defendants maintain that Plaintiffs' pleadings and opposition filings concede that each Cl0p attack on a Progress customer constituted a separate data breach.[10] See [Reply at 4–5]. Defendants point to the Common Complaint's allegation that the software vulnerabilities that

[9] "Plaintiffs must maintain their personal interest in the dispute at all stages of litigation," TransUnion, 594 U.S. at 431, which requires Plaintiffs to demonstrate that standing exists "with the manner and degree of evidence required at the successive stages of the litigation," Webb, 72 F.4th at 371–72 (quoting TransUnion, 594 U.S. at 431). Should facts come out at summary judgment or during bellwether trials that cast doubt on standing, plaintiffs will no longer be entitled to premise standing on "mere allegations." Lujan, 504 U.S. at 561 (citation omitted).

[10] Defendants also contend that because some of "Plaintiffs' original complaints . . . show they view these as separate incidents," including some complaints that did not name all of the entities within the MOVEit Transfer user chain, Plaintiffs cannot now advance factual allegations in the MDL that were lacking in the original complaints. [Reply at 4 n.2 ("Complaints against direct user Defendants routinely did not name Progress and those against VCEs frequently did not name the vendor (or Progress); they named only the VCE.")]. Defendants suggest (without citation) that this is particularly so because "Plaintiffs forced Defendants to pursue their Rule 12(b)(1) motion on the existing complaints rather than file a mass consolidated complaint." [Id.]

The Court ordered (as Defendants are aware) consolidated pleadings to resolve just the issue of standing. MDL Order 13 makes crystal clear that the Common Complaint (filed sixty days before the pending standing motion) would serve as a vehicle for presenting "factual allegations that Plaintiffs contend are relevant to the standing analysis for all parties." [ECF No. 874 at 2 n.1]. Factual allegations concerning the nature of the Cl0p cyberattack not only fit squarely within Order 13, but are precisely the type of "common questions of fact" whose consolidated resolution "will promote the just and efficient conduct" of the pending cases, as contemplated by the MDL statute. 28 U.S.C. § 1407(a).

Cl0p exploited sought to "gain access to each [Progress customer's] server's files without detection." [Id. at 4 (quoting Common Compl. ¶ 139)]. Drawing on the allegation that the vulnerability affected customer servers individually, Defendants ask the Court to infer (unfavorably to Plaintiffs) that the Cl0p attack constituted multiple "unique MOVEit Incident[s] occur[ing] within separate Non-Progress Defendants' environments." [Id.] At the motion-to-dismiss stage, however, the Court must draw all reasonable inferences in favor of Plaintiffs, not Defendants. Taylor, 693 F. Supp. 3d at 97. In any event, the Common Complaint clearly alleges that the intrusion into each customers' servers was hardly "unique," as Defendants contend; rather, Plaintiffs allege that Cl0p exploited just two vulnerabilities common to "[a]ll versions of MOVEit Transfer." [Common Compl. ¶ 132].

The facts plausibly alleged in the Common Complaint adequately support an inference, based on the claim that there was a single breach, that actual misuse of *some* plaintiffs' data means that *all* plaintiffs face a substantial and material risk of future harm. See, e.g., [Common Compl. 249, 279–81]. To be sure, even on Plaintiffs' allegations, the data was stolen from different servers, but that does not necessarily contradict the notion that — as Plaintiffs allege — this was all part of a single breach that exploited vulnerabilities in a single software application, albeit an application that was used in a wide variety of settings. For Defendants' part, they fail to spell out any principle whereby the Court could determine, *a priori*, that the bare fact that compromised data was exfiltrated from multiple servers precludes a plausible allegation that each person whose data was compromised faces a shared risk of future harm.

In arguing that Plaintiffs' allegations of a single breach are insufficient, Defendants place too much weight on this Court's earlier decision in Taylor v. UKG, Inc. In Taylor, the Court held that plaintiffs lacked standing to assert claims related to a data breach, in part because the

Plaintiffs had not alleged actual misuse of their or any other victims' data, nor had they "identified any First Circuit caselaw in which a court has found plaintiffs had established standing in a similar context, without allegations of actual misuse." 693 F. Supp. 3d at 99. Defendants mistakenly read Taylor as erecting a de facto requirement of at least some actual misuse that is found nowhere in Webb. See, e.g., [Reply at 5 ("Taylor, when applied to individual incidents with no misuse allegations, leads to dismissal.")]. Defendants ignore that Webb included an express caveat (which Taylor repeated) that "[the actual misuse] factor, like the others, is not necessarily 'determinative.'"[11] 693 F. Supp. 3d at 99 (quoting Webb, 72 F.4th at 375). This principle is widely accepted across circuits.[12] As the Second Circuit has explained, consistent with Webb, "no court of appeals has explicitly foreclosed plaintiffs from establishing standing based on a risk of future identity theft — even those courts that have declined to find standing on the facts of a particular case." McMorris, 995 F.3d at 300. "Indeed, requiring plaintiffs to allege that they have already suffered identity theft or fraud as the result of a data breach would seem to run afoul of the Supreme Court's recognition that '[a]n allegation of future injury may suffice' to establish Article III standing 'if the threatened injury is certainly impending, or there is a substantial risk that the harm will occur.'" Id. (alteration in original) (quoting Susan B. Anthony List v. Driehaus, 573 U.S. 149, 158 (2014)). Actual misuse is "not a

[11] The plaintiffs in Taylor had failed to advance, and thereby waived, any argument to support why they should be able to assert standing absent an allegation of actual injury. See Mem. in Opp'n, Taylor v. UKG, Inc., No. 22-cv-11168 (D. Mass. Dec. 12, 2022), ECF No. 31. The Court's dismissal in Taylor was a consequence of the plaintiffs' failure to satisfy its burden to show standing. See Hochendoner v. Genzyme Corp., 823 F.3d 724, 731 (1st Cir. 2016). It was not, as Defendants imply, a result of the Court applying a stricter standard to Taylor's claims than that required by Webb. See [Reply at 25].

[12] At least one federal Court has doubted whether a standing analysis is necessary at all when evaluating claims arising under common law tort and contract liability. See generally Clemens, 48 F.4th at 161 (Phipps, J., concurring).

necessary component of establishing standing," even if Courts are "more likely" to find standing where there is some actual misuse. Id. at 301. The Second Circuit even went as far as to indicate that actual misuse is a secondary factor compared to whether the breach deliberately targeted the plaintiffs' data. See id. (describing "whether the data at issue has been compromised as the result of a targeted attack" as the "most important[]" consideration, while specifying that "actual misuse" is "not a necessary component of establishing standing"). Notably, Webb cited McMorris favorably for its analysis of the relationship between actual misuse and future injury. See 72 F.4th at 375–76.

Defendants' assertion that the consolidated cases "retain their separate identities" and must be "evaluated separately" for purposes of standing cannot carry the weight Defendants place on it. See [Reply at 2–4 & n.2 (quoting Gelboim v. Bank of Am. Corp., 574 U.S. 405, 413 (2015))]. MDL consolidation often bears on the adjudication of Article III standing. See In re Equifax, Inc. Customer Data Sec. Breach Litig., 289 F. Supp. 3d 1322, 1325 (J.P.M.L. 2017) ("[T]he Panel does not consider the possible implications with respect to standing or other potential rulings when it selects a transferee district."). Although the MDL transfer statute does not automatically "imbu[e] transferred actions with some new and distinctive . . . character," Lexecon Inc. v. Milberg Weiss Bershad Hynes & Lerach, 523 U.S. 26, 37 (1998), the Supreme Court has made clear that consolidation may lead transferee courts to examine facts and allegations in the aggregate, Gelboim, 574 U.S. at 413 (noting that transferred cases "ordinarily retain their separate identities" (emphasis added)). In particular, the Court has noted that when parties in an MDL agree to file a "master complaint," that filing may "supersede prior individual pleadings." Id. at 413 n.3 (quoting In re Refrigerant Compressors Antitrust Litig., 731 F.3d 586, 590–92 (6th Cir. 2013)). A transferee court may even "treat the master pleadings as merging the

discrete actions for the duration of the MDL pretrial proceedings." Id. (quoting Refrigerant Compressors, 731 F.3d at 590–92). Once a master complaint is filed, as long as the cases remain pending in the MDL, they are, for purposes of the transferee court, a "single action." Refrigerant Compressors, 731 F.3d at 589.

In this case, the Common Complaint does not go so far as to merge and consolidate the cases pending in this MDL, but the parties' joint proposal explicitly contemplated that new, common allegations included in the pleadings could serve as a basis for asserting standing. See [ECF No. 851 at 1, 4 (explaining that the omnibus standing motion would respond to the individual complaints "plus . . . a set of designated additional, common allegations upon which plaintiffs intend to rely in responding to any Article III standing challenge")]; cf. In re Nuvaring Prods. Liab. Litig., No. 08-md-01964, 2009 WL 2425391, at *2 (E.D. Mo. Aug. 6, 2009) (explaining that consolidated complaint was merely an "administrative tool" when neither the district court nor the parties "contemplated that Rule 12(b) motion practice would be pursued . . . against the master complaint"). Gelboim confirms the Courts' view that the Court can — and in light of MDL Order No. 13, must — look at common pleadings and the individual complaints in aggregate to measure standing. With this in mind, the Court finds that because a significant number of Plaintiffs (between 30 and 157 of the more than 300 Plaintiffs in this case) allege actual misuse of their data after the Data Breach, the Plaintiffs plausibly allege that the breach substantially and materially increased the risk of future harm for all Plaintiffs.

iii. Factor Three: Whether the stolen data was highly sensitive.

The third factor requiring consideration under Webb is "whether the type of data that has been exposed is sensitive such that there is a high risk of identity theft or fraud." Webb, 72 F.4th at 375 (quoting McMorris, 995 F.3d at 303). Defendants do little to parry Plaintiffs' allegations

on this score. Defendants note generally that "[t]he sensitivity of the impacted data elements varied by Defendant" and they point out that "[n]umerous Plaintiffs do not allege that any sensitive personal information was affected."[13] [Mot. at 22].

Plaintiffs assert that 381 Plaintiffs had their social security numbers, financial information, or protected health information compromised in the breach, as well as other personally identifiable information. [Opp'n at 29–30]. But, looking to the First Circuit's guidance, such variations in what information was stolen (even the absence of specific allegations identifying what data was stolen), do not defeat standing. Notably, in Webb, Plaintiff Charley satisfied the injury-in-fact element even though she was unable to offer specific allegations concerning what data had been lost in the IWP data breach. 72 F.4th at 370 ("[Charley] called IWP to confirm that her information was stolen, but IWP's representatives would not provide her with specific details as to what types of information were accessed."). In the Court's view, it suffices that "at least some" — and per Plaintiffs' allegations, much — "of the stolen data was highly sensitive." In re LastPass Data Sec. Incident Litig., --- F. Supp. 3d ---, No. 22-cv-12047, 2024 WL 3580646, at *5 (D. Mass. July 30, 2024).

d. Whether Plaintiffs have alleged separate, concrete, present injuries.

"To have standing to pursue damages based on a risk of future harm, plaintiffs must demonstrate a separate concrete harm caused 'by their exposure to the risk itself.'" Webb, 72 F.4th at 372 (quoting TransUnion, 594 U.S. at 437). Plaintiffs contend that they have alleged

[13] Citing this Court's decision in Taylor, Defendants also note that merely "alleg[ing] that . . . more sensitive personal data (e.g., Social Security numbers) w[ere] accessed . . . does not necessarily confer standing." [Mot. at 22–23]. In Taylor, though, the Court made clear that the decision in that case turned on the absence of "allegations of actual misuse," not on the sensitivity of the data. 693 F. Supp. 3d at 99.

multiple separate, concrete harms,[14] including mitigation efforts, lost time, and emotional damages caused by their exposure to the imminent risk of future harm (i.e., the risk of future identity theft or fraud).[15] See id. Based on the foregoing analysis, the Court concludes that all Plaintiffs have adequately alleged separate, concrete injuries sufficient to support their standing to seek damages.

1. Mitigation efforts and lost time

It is well established that "'[t]ime spent responding to a data breach can constitute a concrete injury sufficient to confer standing' where the 'time would otherwise have been put to profitable use' and it was spent in 'response to a substantial and imminent risk of harm.'" LastPass, 2024 WL 3580646, at *4 (quoting Webb, 72 F.4th at 377). The allegations in the Common Complaint regarding mitigation are much like those in the Equifax litigation, where the court noted, Plaintiffs have engaged in proactive and reactive mitigation efforts, such as "purchasing credit freezes and monitoring services, and spending hours reviewing financial accounts — allegations sufficient to confer standing in claiming damages." In re Fortra File Transfer Software Data Sec. Breach Litig., --- F. Supp. 3d ----, 2024 WL 4547212, at *5 (S.D. Fla. Sept. 18, 2024).

[14] Plaintiffs also contend that these injuries satisfy the particularization requirement, and the Court agrees. Each Plaintiff's allegations of lost time and emotional distress constitute allegations that they have "been affected 'in a personal and individual way.'" Hochendoner v. Genzyme Corp., 823 F.3d 724, 732 (1st Cir. 2016) (citation omitted). The fact that many of the plaintiffs allege they have suffered such injuries does not convert their allegations into a "generalized grievance," Lyman v. Baker, 954 F.3d 361 (1st Cir. 2020), so long as their personal experience supports the allegation.

[15] Although the Common Complaint refers to further injuries based on Plaintiffs' loss of the benefit of their bargain and loss of value of their PII, see [Common Compl. ¶¶ 240, 277], they do not advance these theories in their opposition papers, see [Opp'n at 31 n.15].

Defendants ask that the Court disregard the Plaintiffs' mitigation efforts as a mere attempt to "manufacture standing merely by inflicting harm on themselves." [Mot. at 26 (quoting Clapper, 568 U.S. at 409)]; see also [Reply at 10]. This line of argument, however, only makes sense if there is a failure to allege a substantial risk of future harm. In the Common Complaint, however, the risk of substantial harm is adequately pleaded. As discussed above, Defendants suggest that Plaintiffs should take solace in the prospect that the sophisticated criminals who executed the data breach are mainly in the ransom business, rather than the identity theft business. But, on the face of the plausible allegations of the Common Complaint, there appears to have been little if any way for Plaintiffs to identify which particular individuals' stolen information would be misused. In other words, because "Plaintiffs have plausibly shown they face a real and imminent threat of misuse of their data," "their lost time" and related mitigation efforts — including paying for credit monitoring and other identity protections — "constitutes injury in fact." LastPass, 2024 WL 3580646, at *5. As the First Circuit has explained in the context of a data breach, "the test for mitigation is not hindsight." See Anderson v. Hannaford Bros. Co., 659 F.3d 151, 165 (1st Cir. 2011); see also Webb, 72 F.4th at 373 n.4 (describing Anderson as "instructive" on the question of reasonable mitigation).

2. Emotional Distress

Plaintiffs also maintain that their alleged emotional injuries caused by their exposure to an increased risk of harm provide a separate, concrete injury. [Opp'n at 33–34]. Although Webb did not need to address whether emotional distress could, by itself, suffice to allege an additional, present harm for standing purposes, Plaintiffs point out that several courts have recognized that "if the plaintiff's knowledge of the substantial risk of identity theft causes him to presently experience emotional distress . . . , the plaintiff has alleged a concrete injury."

Clemens, 48 F.4th at 156. The Supreme Court nodded to this theory of concrete injury, albeit in dicta, in TransUnion itself. 594 U.S. at 436 n.7 (suggesting that "a Plaintiff's knowledge that he or she is exposed to a risk of future . . . harm could cause its own current emotional or psychological harm"); see also United Nurses & Allied Pros. v. NLRB, 975 F.3d 34, 40 (1st Cir. 2020) (noting that lower courts are "bound by the Supreme Court's 'considered dicta' . . . particularly when . . . [it] is of recent vintage and not enfeebled by any subsequent statement" (quoting McCoy v. Mass. Inst. of Tech., 950 F.2d 13, 19 (1st Cir. 1991)). Although Defendants point to post-TransUnion precedent denying standing premised on emotional distress, the cases they cite did not include allegations of a risk of future harm. Baysal v. Midvale Indem. Co., 78 F.4th 976, 978–79 (7th Cir. 2024) (holding emotional distress could not provide concrete injury in breach involving loss of drivers' license numbers). Although this Court previously held in Scifo that "conclusory statements" alone cannot establish emotional harm as a concrete injury supporting standing, Scifo, 2024 WL 4252694, at *5 n.9, Scifo too is distinguishable on the same ground. Because the Court had found that the Plaintiffs in that case had not alleged an increased risk of future harm, see id., their allegations of emotional distress were not in response to "knowledge that [they were] exposed to" such a risk and, thus, were merely conclusory, TransUnion, 594 U.S. at 436 n.7. As another district court considering such arguments explained:

> These cases are markedly different from this action. Here, Plaintiffs have established that their risk of future harm is substantial and imminent. Thus, the question in this case is not whether Plaintiffs' allegations of emotional distress, on their own, are sufficiently concrete to establish injuries in fact. Instead, it is whether allegations of emotional distress, coupled with the substantial risk of future harm, are sufficiently concrete to establish standing in a claim for damages.

In re Mednax Servs., Inc., Customer Data Sec. Breach Litig., 603 F. Supp. 3d 1183, 1203 (S.D. Fla. 2022). The Court thus concludes that those Plaintiffs who allege emotional distress (and have pled related costs) have adequately alleged an independent concrete harm sufficient to support standing for damages.

e. Traceability

In addition to pleading a redressable injury, plaintiffs asserting federal standing must also plausibly allege that their injury is "'fairly traceable' to the challenged action of the defendant." Lujan, 504 U.S. at 560 (cleaned up). "The 'traceability' or causation element 'requires the plaintiff to show a sufficiently direct causal connection between the challenged action and the identified harm.'" Dantzler, Inc. v. Empresas Berríos Inventory & Operations, LLC, 958 F.3d 38, 47 (1st Cir. 2020) (quoting Katz, 672 F.3d at 71). Traceability is not the same as "[p]roximate causation." Webb, 72 F.4th at 377 (quoting Lexmark Int'l, Inc. v. Static Control Components, Inc., 572 U.S. 118, 134 n.6 (2014)). In the context of a data breach, an injury is "'fairly traceable' to a defendant's conduct for the purposes of Article III standing if plaintiffs plausibly allege the defendant's 'actions led to the exposure and actual or potential misuse'" of plaintiffs PII or PHI. LastPass, 2024 WL 3580646, at *5 (quoting Webb, 72 F.4th at 377).

Plaintiffs here have plausibly alleged that the exposure of their data to Cl0p, which created an actual or potential risk of misuse, is fairly traceable to Defendants' actions vis-à-vis the Data Breach. Plaintiffs set forth extensive allegations of prophylactic cybersecurity measures that, they allege, should have been undertaken by Defendants in anticipation of a ransomware incident like the Data Breach, and which would have prevented it. [Common Compl. ¶¶ 282–313]. Allegations that defendants failed to adequately safeguard data and thereby subjected

plaintiffs to a substantial risk of identity theft and other harm is sufficient for Article III purposes. Attias, 865 F.3d at 629; Webb, 72 F.4th at 377.

Defendants offer four arguments to support their contention that the Common Complaint allegations are insufficient to plausibly show traceability. First, Defendants contend that the injuries alleged by some of the actual-misuse Plaintiffs lack a plausible causal relationship to the types of data Plaintiffs allege were stolen. See [Mot. at 37–38, 44 n.27]. Defendant's analysis, which is not laid out clearly in its motion or its filed appendices, appears to be incomplete. Plaintiffs point out, and the Court's examination of the underlying individual complaints confirms, that many of Defendants' examples do not amount to the sort of complete data mismatches that could defeat traceability. For instance, Defendants contend that Jose Vargas's allegations that the Data Breach caused "an increase in spam calls, texts, and/or emails" are implausible because Vargas does not claim that the incident involved his phone number or email address (and does not otherwise explain how the Data Breach could have resulted in increased calls, texts or emails). [Reply at 14 (quoting First Am. Compl. ("Walles Compl.") ¶¶ 140, 144, Walles v. AutoZone, Inc., No. 23-cv-12889, (D. Mass. Dec. 5, 2023), ECF No. 6)]. This, however, overlooks Vargas's well-pleaded allegations of identify fraud as evidenced by (1) an unauthorized person applying for a loan in his name in November 2023, and (2) AutoZone's data breach notice informing him that his Social Security number was disclosed in the Data Breach and connected to his full name. [Walles Compl. ¶¶ 7, 11, 34, 192, 224, 252]. Thus, even if one of Vargas's alleged injuries may run into a data mismatch, he has alleged a separate, traceable injury that allows the Court to exercise jurisdiction.

More broadly, Defendants' "data match" argument may raise significant factual issues, but, as a matter of law, it does not foreclose plausible allegations of harm sufficient to establish

standing. Other courts have reached the same conclusion. "Even if the data accessed in the Data Breach[] did not provide all the information necessary to inflict [some of the] harms [Plaintiffs' allege]," where the breach has included sensitive PII, like SSNs and DOBs, that data "very well could have been enough to aid therein." Mednax, 603 F. Supp. 3d at 1206; [Walles Compl. ¶¶ 93–100 (making such allegations)]. "Even a showing that a plaintiff's injury is indirectly caused by a defendant's actions satisfies the fairly traceable requirement." Resnick v. AvMed, Inc., 693 F.3d 1317, 1324 (11th Cir. 2012). It is worth noting, as well, that even in a case of total data mismatch — which would undercut a particular plaintiff's claim of actual injury — the plaintiff would still be able to assert standing based on a substantial risk of future harm for the reasons set forth supra.

Second, Defendants contend that any allegations of injury that predate August 15, 2023, cannot be fairly traceable to the Data Breach because that is the date on which Plaintiffs allege Cl0p began disclosing stolen data. [Mot. at 38–41]. Here, Defendants are on firmer ground. The Court agrees that allegations of actual misuse that predate the disclosure of the stolen information fail to satisfy the traceability requirement for standing. See Scifo, 2024 WL 4252694, at *3. But for the reasons discussed supra, even Plaintiffs whose allegations of *actual* misuse fail for this reason may still assert standing based on a traceable, substantial risk of future harm traceable to the breach. On the other hand, the Court agrees with Defendants that the four Plaintiffs whose individual complaints were filed prior to August 15, 2023, cannot plausibly assert actual misuse that is traceable to the Data Breach, since "[j]urisdiction depends upon the facts as they existed when the complaint was brought." Sallen v. Corinthians Licenciamentos LTD A, 273 F.3d 14, 23 (1st Cir. 2001). The Court agrees the allegations in the Common Complaint do not provide a basis to conclude that Plaintiffs were at an increased risk of future

harm before any traceable actual misuse plausibly could have occurred. Consequently, such actions are dismissed, as set forth in the Appendix.

Third, Defendants contend that Plaintiffs have not presented allegations that would subject either the Vendor Contracting Entity ("VCE") or Vendor Contracting Entity Customers ("VCEC") to liability. [Mot. at 42–43]. Defendants insist that because the cyberattack targeted Vendors' servers, and not the servers of the VCEs and VCECs, "no amount of cybersecurity by these Defendants . . . could have prevented the MOVEit Incident[] from occurring." [Id.] Defendants further maintain that "where Plaintiffs do allege inadequate oversight, Plaintiffs fail to link Plaintiffs' alleged harm to these Defendants because Progress was not their vendor." [Id.]. At the Rule 12(b)(1) stage, however, Plaintiffs' claim that adequate vendor/third-party risk management programming at the VCE/VCEC level would have prevented the Data Breach — though it may prove insufficient to establish liability at subsequent stages of the MDL[16] — adequately alleges for present purposes that Plaintiffs' injuries are fairly traceable, at least in part, to the actions of those parties. Lujan, 504 U.S. at 561 (courts presume that "general factual allegations of injury resulting from the defendant's conduct . . . embrace those specific facts that are necessary to support the claim"); accord Webb, 72 F.4th at 374. This is particularly so given that Plaintiffs specifically allege that the Data Breach was enabled by "common attack vectors, including SQL Injection susceptibility." [Common Compl. ¶ 433]. In other words, Plaintiffs have plausibly alleged that, in the absence of adequate vetting protocols, "third parties" (here, Cl0p) would "likely react in predictable ways," i.e., by exploiting vulnerabilities in their

[16] Whether Plaintiffs have plausibly alleged causal links that could support VCE/VCEC liability is not a question properly before the Court on a Rule 12(b)(1) motion. "It is firmly established . . . that the absence of a valid . . . cause of action does not implicate subject-matter jurisdiction, i.e., the courts' statutory or constitutional power to adjudicate the case." Steel Co. v. Citizens for a Better Env't, 523 U.S. 83, 89 (1998).

upstream business partners' security configurations. California v. Texas, 593 U.S. 659, 675 (2021) (quoting Dep't of Comm. v. New York, 588 U.S. 752, 768 (2019)). "Article III standing does not require that the defendant be the most immediate cause, or even a proximate cause, of the plaintiffs' injuries; it requires only that those injuries be 'fairly traceable' to the defendant." Attias, 865 F.3d at 629.

Fourth and last, Defendants argue that Plaintiffs' allegations are insufficient to show traceability because, in Defendants' telling, "there is a strong probability that much of the information stolen in the Data Breach has not yet been made available on the black market in a coherent, organized fashion." [Mot. (quoting Common Compl. ¶ 251)]. This too is a factual contention that is not ripe for consideration at the pleading stage. Plaintiffs have plausibly alleged that their sensitive data has been exfiltrated and that (some of) that data has been posted to the web. Whether Defendants can ultimately establish that this is a "no-harm/no-foul" situation cannot be determined at this stage. Thus, Plaintiffs' claims suffice to support standing.

In particular, Defendants argue that to rearrange the data in a coherent, organized fashion — i.e., in a manner that would let black-market buyers misuse it — would "depend[] on actions of third parties." [Id. (quoting Dantzler, 958 F.3d at 48)]. "By alleging that the published data was ***not*** available 'in a coherent, organized fashion' . . . Plaintiffs raise yet additional steps required of any third party that might have sought to exploit Cl0p's work . . . ." [Id. (quoting Common Compl. ¶ 251)]. Defendants' characterization removes Plaintiffs' allegation from the context in which it was made. The Common Complaint alleges that because of "a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used," it is likely that for many class members, their data may not yet have "been made available on the black market in a coherent, organized fashion," making it difficult

for class members to determine what information has been stolen. [Common Compl. ¶¶ 250–51]. Drawing reasonable inferences in Plaintiffs favor, the Court easily concludes that sophisticated bad actors are capable of misusing troves of data on dark web, even when such data has been disseminated only in unstructured form, such that it might be difficult for ordinary internet users to do the same. As such, Plaintiffs have plausibly alleged that bad actors have reacted already and will "likely react in predictable ways" to the publication of raw PII and PHI on the dark web. California, 593 U.S. at 676 (quoting Dep't of Comm., 588 U.S. at 768). In sum, even though "much of the information stolen in the Data Breach has not yet been made available on the black market," non-misuse Plaintiffs nonetheless face a risk of future harm traceable to the Data Breach.

Thus, for the foregoing reasons, the Court concludes that all but the four Plaintiffs in the cases identified below have alleged traceable injuries supporting Article III standing.

IV. CONCLUSION

For the reasons set forth, Defendants' motion to dismiss, [ECF No. 1114], is **GRANTED IN PART** and **DENIED IN PART**. The individual cases dismissed due to a lack of traceable injury are: Harris v. Progress Software Corp., No. 23-cv-11816; Oakwood v. Corebridge Financial, Inc., No. 23-cv-12643; Newman v. Corebridge Financial Inc., No. 23-cv-12649; and O'Neal v. Lumico Life Insurance Co., No. 24-cv-10078.

December 12, 2024

/s/ *Allison D. Burroughs*
ALLISON D. BURROUGHS
U.S. DISTRICT JUDGE

APPENDIX

For the reasons explained in footnote 3, the requests for injunctive relief in the cases associated with the following case numbers are dismissed for lack of standing.

- 1:23-cv-07822
- 1:23-cv-10035
- 1:23-cv-11370
- 1:23-cv-11412
- 1:23-cv-11442
- 1:23-cv-11543
- 1:23-cv-11552
- 1:23-cv-11669
- 1:23-cv-11782
- 1:23-cv-11816
- 1:23-cv-11864
- 1:23-cv-11913
- 1:23-cv-11931
- 1:23-cv-11939
- 1:23-cv-11984
- 1:23-cv-12010
- 1:23-cv-12015
- 1:23-cv-12028
- 1:23-cv-12067
- 1:23-cv-12127
- 1:23-cv-12156
- 1:23-cv-12157
- 1:23-cv-12192
- 1:23-cv-12202
- 1:23-cv-12203
- 1:23-cv-12255
- 1:23-cv-12273
- 1:23-cv-12275
- 1:23-cv-12281
- 1:23-cv-12300
- 1:23-cv-12342
- 1:23-cv-12356
- 1:23-cv-12362

- 1:23-cv-12363
- 1:23-cv-12411
- 1:23-cv-12412
- 1:23-cv-12416
- 1:23-cv-12423
- 1:23-cv-12424
- 1:23-cv-12426
- 1:23-cv-12427
- 1:23-cv-12432
- 1:23-cv-12435
- 1:23-cv-12438
- 1:23-cv-12440
- 1:23-cv-12441
- 1:23-cv-12445
- 1:23-cv-12447
- 1:23-cv-12448
- 1:23-cv-12449
- 1:23-cv-12450
- 1:23-cv-12451
- 1:23-cv-12453
- 1:23-cv-12472
- 1:23-cv-12473
- 1:23-cv-12476
- 1:23-cv-12478
- 1:23-cv-12481
- 1:23-cv-12483
- 1:23-cv-12484
- 1:23-cv-12485
- 1:23-cv-12486
- 1:23-cv-12488
- 1:23-cv-12489
- 1:23-cv-12490
- 1:23-cv-12492
- 1:23-cv-12495
- 1:23-cv-12496
- 1:23-cv-12497
- 1:23-cv-12500
- 1:23-cv-12501

- 1:23-cv-12506
- 1:23-cv-12507
- 1:23-cv-12508
- 1:23-cv-12512
- 1:23-cv-12514
- 1:23-cv-12515
- 1:23-cv-12524
- 1:23-cv-12554
- 1:23-cv-12560
- 1:23-cv-12561
- 1:23-cv-12565
- 1:23-cv-12567
- 1:23-cv-12568
- 1:23-cv-12570
- 1:23-cv-12571
- 1:23-cv-12572
- 1:23-cv-12573
- 1:23-cv-12590
- 1:23-cv-12591
- 1:23-cv-12592
- 1:23-cv-12593
- 1:23-cv-12598
- 1:23-cv-12599
- 1:23-cv-12601
- 1:23-cv-12602
- 1:23-cv-12603
- 1:23-cv-12627
- 1:23-cv-12634
- 1:23-cv-12649
- 1:23-cv-12656
- 1:23-cv-12657
- 1:23-cv-12658
- 1:23-cv-12659
- 1:23-cv-12667
- 1:23-cv-12669
- 1:23-cv-12670
- 1:23-cv-12710
- 1:23-cv-12736

- 1:23-cv-12762
- 1:23-cv-12764
- 1:23-cv-12765
- 1:23-cv-12766
- 1:23-cv-12767
- 1:23-cv-12768
- 1:23-cv-12769
- 1:23-cv-12771
- 1:23-cv-12772
- 1:23-cv-12773
- 1:23-cv-12774
- 1:23-cv-12780
- 1:23-cv-12781
- 1:23-cv-12785
- 1:23-cv-12786
- 1:23-cv-12787
- 1:23-cv-12788
- 1:23-cv-12790
- 1:23-cv-12816
- 1:23-cv-12836
- 1:23-cv-12858
- 1:23-cv-12860
- 1:23-cv-12861
- 1:23-cv-12863
- 1:23-cv-12866
- 1:23-cv-12870
- 1:23-cv-12871
- 1:23-cv-12874
- 1:23-cv-12875
- 1:23-cv-12876
- 1:23-cv-12884
- 1:23-cv-12885
- 1:23-cv-12887
- 1:23-cv-12889
- 1:23-cv-12891
- 1:23-cv-12892
- 1:23-cv-12893
- 1:23-cv-12894

- 1:23-cv-12897
- 1:23-cv-12898
- 1:23-cv-12899
- 1:23-cv-12903
- 1:23-cv-12910
- 1:23-cv-12922
- 1:23-cv-12968
- 1:23-cv-12974
- 1:23-cv-12976
- 1:23-cv-12977
- 1:23-cv-12981
- 1:23-cv-12982
- 1:23-cv-12983
- 1:23-cv-12985
- 1:23-cv-12986
- 1:23-cv-12994
- 1:23-cv-12996
- 1:23-cv-13022
- 1:23-cv-13025
- 1:23-cv-13027
- 1:23-cv-13029
- 1:23-cv-13037
- 1:23-cv-13038
- 1:23-cv-13052
- 1:23-cv-13054
- 1:23-cv-13057
- 1:23-cv-13058
- 1:23-cv-13059
- 1:23-cv-13062
- 1:23-cv-13064
- 1:23-cv-13066
- 1:23-cv-13070
- 1:23-cv-13071
- 1:23-cv-13072
- 1:23-cv-13077
- 1:23-cv-13079
- 1:23-cv-13080
- 1:23-cv-13097

- 1:23-cv-13098
- 1:23-cv-13231
- 1:23-cv-13233
- 1:24-cv-10022
- 1:24-cv-10031
- 1:24-cv-10034
- 1:24-cv-10038
- 1:24-cv-10059
- 1:24-cv-10068
- 1:24-cv-10069
- 1:24-cv-10070
- 1:24-cv-10073
- 1:24-cv-10074
- 1:24-cv-10078
- 1:24-cv-10177
- 1:24-cv-10183
- 1:24-cv-10186
- 1:24-cv-10204
- 1:24-cv-10205
- 1:24-cv-10206
- 1:24-cv-10207
- 1:24-cv-10214
- 1:24-cv-10215
- 1:24-cv-10218
- 1:24-cv-10251
- 1:24-cv-10261
- 1:24-cv-10418
- 1:24-cv-10581
- 1:24-cv-10584
- 1:24-cv-10586
- 1:24-cv-10589
- 1:24-cv-10618
- 1:24-cv-10636
- 1:24-cv-10641
- 1:24-cv-10645
- 1:24-cv-10657
- 1:24-cv-10664
- 1:24-cv-10668

- 1:24-cv-10671
- 1:24-cv-10673
- 1:24-cv-10679
- 1:24-cv-10684
- 1:24-cv-10783
- 1:24-cv-10784
- 1:24-cv-10813
- 1:24-cv-10844
- 1:24-cv-10929
- 1:24-cv-11012
- 1:24-cv-11068
- 1:24-cv-11070
- 1:24-cv-11126
- 1:24-cv-11127
- 1:24-cv-11281
- 1:24-cv-11359
- 1:24-cv-11368
- 1:24-cv-11372
- 1:24-cv-11511
- 1:24-cv-11523
- 1:24-cv-11541
- 1:24-cv-11558
- 1:24-cv-11566
- 1:24-cv-11567
- 1:24-cv-11574
- 1:24-cv-11575
- 1:24-cv-11701
- 1:24-cv-11702
- 1:24-cv-11763
- 1:24-cv-11807
- 4:23-cv-40158